Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claim 1 (currently amended): A user authentication system, comprising:

a data holding medium for holding a common key ~~unique to~~ corresponding to a user, used in a common-key encryption method for authentication between the data holding medium held by the user and an authentication apparatus~~, and a private key used in a public-key encryption method to the authentication between the data holding medium and a server to perform a service to the user~~;

said authentication apparatus for holding the common key used in the common-key encryption method and a private key corresponding to the user used in a public-key encryption method for authentication between the data holding medium and a server to perform a service to the user~~, each unique to the user~~; and

an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for performing authentication by the public-key encryption method;

wherein said authentication apparatus is configured to receive a first data item, wherein the first data item is associated with a first authentication request from said information processing apparatus, and wherein said authentication apparatus is configured to authenticate the data holding medium by using the common key in response to the first authentication request;

wherein said authentication apparatus is further configured to encrypt, only if the data holding medium is authenticated in response to the first authentication request, the first data item using the private key associated with the user and to send the encrypted first data item to the information processing apparatus;

wherein said information processing apparatus is configured to decrypt the encrypted first data item using a public key associated with the user and to compare the decrypted result with the first data item;

wherein the authentication apparatus performs authentication, authenticating the data holding medium by using the common key used in the common-key encryption method for the user held by the data holding medium, in response to an additional authentication request sent from the information processing apparatus, wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item, and

wherein, only when the user has been authenticated in response to the additional authentication request, the authentication apparatus performs processing, using the private key corresponding to the user, for making the information processing apparatus authenticate the user ~~by using the private key corresponding to the user~~,

wherein information encrypted by the public-key encryption method, which is sent from the information processing apparatus~~,~~ and forwarded to the authentication apparatus, is decrypted by the authentication apparatus using the private key corresponding to the user so as to obtain decrypted information;

wherein the decrypted information is encrypted ~~means~~ by the authentication apparatus using the common key; and

wherein the obtained common key encrypted information is sent back to the data holding medium.

Claim 2 (original): An authentication system as claimed in Claim 1, wherein the data holding medium is portable.

Claim 3 (original): An authentication system as claimed in Claim 1, wherein the information processing apparatus is a mobile communication apparatus.

Claim 4 (original): An authentication system as claimed in Claim 1, wherein the data holding medium and the information processing apparatus are integrated as a unit.

Claim 5 (currently amended): A user authentication method for a user who carries a data holding apparatus for holding a common key ~~unique to~~ of a user, used in a common-key encryption method for authentication of the data holding apparatus held by the user and an

authentication apparatus for authentication between the data holding apparatus and a server to perform a service to the user, the method comprising the steps of:

authenticating the data holding apparatus of the user by the common-key encryption method by using the common key held by the data holding apparatus in response to an authentication request from the server;

receiving a first data item, wherein the first data item is associated with the authentication request from the server; ~~and~~

performing, only when the data holding apparatus of the user has been authenticated, processing for authenticating the data holding apparatus of the user by a public-key encryption method, wherein the processing includes encrypting the first data item using a private-key of the user and sending the encrypted first data item to the server, wherein the server decrypts the encrypted first data item using a public-key of the user and compares the decryption result with the first data item;

receiving a second data item, wherein the second data item is encrypted by the server using the public-key of the user;

decrypting the second data item using the private-key of the user;

encrypting the decrypted second data item using the common key; and

sending the result of encrypting the decrypted second data item to the data holding apparatus.

Claim 6 (original): A user authentication method as Claimed in Claim 5, wherein the data holding medium is portable.

Claim 7 (original): A user authentication method as claimed in Claim 5, wherein the user authentication request is sent from an information processing apparatus.

Claim 8 (original): A user authentication method as claimed in Claim 7, wherein the information processing apparatus and the data holding apparatus are integrated as a unit.

Claim 9 (original): A user authentication method as claimed in Claim 7, wherein the information processing apparatus has a communication function.

Claim 10 (original): A user authentication method as claimed in Claim 5, wherein the data holding apparatus is an IC card.

Claim 11 (original): A user authentication method as claimed in Claim 9, wherein the data holding apparatus is an IC card.

Claim 12 (original): A user authentication method as claimed in Claim 11, wherein the information processing apparatus has a communication function, a browser function for accessing information on the Internet, and a reader and writer function for reading and writing the IC card.

Claim 13 (currently amended): An authentication method, comprising the steps of:

holding a common key ~~unique to~~ corresponding to a user used in a common-key encryption method for authentication between a data holding apparatus held by the user and an authentication apparatus, and a private key used in a public-key encryption method ~~to the~~ for authentication between the data holding apparatus and a server to perform a service to the user;

receiving a first data item, wherein the first data item is associated with a first authentication request from the server;

performing, only when the data holding apparatus of the user has been authenticated in response to the first authentication request, processing for authenticating the data holding apparatus of the user by a public-key encryption method, wherein the processing includes encrypting the first data item using a private-key of the user and sending the encrypted first data item to the server, wherein the server decrypts the encrypted first data item using a public-key of the user and compares the decryption result with the first data item;

authenticating, in response to an additional authentication request sent from an external information processing apparatus, the data holding apparatus by using the held common key used in the common-key encryption method for the user ~~held by the data holding apparatus~~; and

performing, only when the data holding apparatus has been authenticated in response to the additional authentication request in the authentication step, processing, using the private key corresponding to the user, for making the information processing apparatus authenticate the data holding apparatus by the public-key encryption method ~~by using the private key corresponding to the user~~,

wherein~~,~~ information encrypted by the public-key encryption method, which is sent from the server~~,~~ and forwarded to the authentication apparatus, is decrypted by an authentication device using the private key corresponding to the user so as to obtain decrypted information;

wherein the decrypted information is encrypted ~~means~~ using the common key; and

wherein the obtained common key encrypted information is sent back to the data holding apparatus.

Claim 14 (currently amended): An authentication apparatus, comprising:

a holder for holding a common key ~~unique to~~ corresponding to a user, used in a common-key encryption method for authentication between a data holding medium held by the user and an authentication apparatus, and a private key used in a public-key encryption method ~~to the~~ for authentication between the data holding medium and a server to perform a service to the user;

an authenticating device configured to receive a first data item, wherein the first data item is associated with a first authentication request from said server, and wherein said authenticating device is configured to authenticate the data holding medium by using the common key in response to the first authentication request;

wherein said authenticating device is further configured to encrypt, only if the data holding medium is authenticated in response to the first authentication request, the first data item using the private key associated with the user and to send the encrypted first data item to the server;

wherein said server is configured to decrypt the encrypted first data item using a public key associated with the user and to compare the decrypted result with the first data item;

wherein said authenticating device is further configured for, in response to an additional authentication request sent from the server, authenticating the data holding medium by using the common key used in common-key encryption method for the user ~~held by the data holding medium~~, wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item, and

wherein said authenticating device is further configured for, only when the data holding medium has been authenticated in response to the additional authentication request~~,~~ by using the common keys, performing, using the private key corresponding to the user, a processing for authenticating between the data holding medium and the server ~~by using the private key corresponding to the user~~,

wherein information encrypted by the public-key encryption method, which is sent from the server~~,~~ and forwarded to the authentication apparatus, is decrypted by the authentication device using the private key corresponding to the user so as to obtain decrypted information;

wherein the decrypted information is encrypted ~~means~~ using the common key; and

wherein the obtained common key encrypted information is sent back to the data holding medium.

Claim 15 (original): An authentication apparatus as claimed in Claim 14, wherein the authentication apparatus has a private key used in the public-key encryption method.

Claim 16 (original): An authentication apparatus as claimed in Claim 14, wherein the data holding medium is an IC card.

Claim 17 (original): An authentication apparatus as claimed in Claim 16, wherein the information processing apparatus has a reader and writer function for reading and writing the IC card.

Claim 18 (original): An authentication apparatus as claimed in Claim 14, wherein the data holding medium is integrated with the information processing apparatus as a unit.

Claim 19 (original): An authentication apparatus as claimed in Claim 14, wherein the information processing apparatus is a mobile communication apparatus.

Claim 20 (original): An authentication apparatus as claimed in Claim 19, wherein the information processing apparatus has a communication function, and a browser function for accessing information on the Internet.

Claim 21 (currently amended): A user authentication system~~, wherein a data holding medium for holding a common key unique to a user, used in a common key encryption method~~, comprising:

a data holding medium for holding a common key associated with a user;

a server for sending ~~an~~ a plurality of authentication requests to perform a service to the user; and

an authentication apparatus comprising,

a holding means for holding the common key corresponding to the user used in a common-key encryption method for authentication between a data holding medium held by the user and the authentication apparatus, said holding means holding a private key used in a public-key encryption method ~~to the~~ for authentication between the data holding medium and the server;

means for authenticating wherein said means for authenticating is configured to receive a first data item, wherein the first data item is associated with a first authentication request from said server, and wherein said means for authenticating is configured to authenticate the data holding medium by using the common key in response to the first authentication request;

wherein said means for authenticating is further configured to encrypt, only if the data holding medium is authenticated in response to the first authentication request, the first data item using the private key associated with the user and to send the encrypted first data item to the server;

wherein said server is configured to decrypt the encrypted first data item using a public key associated with the user and to compare the decrypted result with the first data item;

wherein the means for authenticating is further configured to authenticate the data holding medium by using the common key used in common-key encryption method for the user ~~held by the data holding medium~~ in response to ~~the~~ an additional authentication request sent from the server, wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item,

said authenticating means performing, using the private key corresponding to the user, a processing for authentication between the data holding medium and the server ~~by using the private key corresponding to the user~~ when the data holding medium has been authenticated by using the common keys in response to the additional authentication request,

wherein information encrypted by the public-key encryption method, which is sent from the server~~,~~ and forwarded to the authentication apparatus, is decrypted by the authentication device using the private key corresponding to the user so as to obtain decrypted information;

wherein the decrypted information is encrypted ~~means~~ using the common key; and

wherein the obtained common key encrypted information is sent back to the data holding medium.

Claim 22 (currently amended): An authentication method between a data holding medium and a server by an authentication apparatus, said data holding medium holding a common key ~~unique to~~ corresponding to a user, used in a common-key encryption method, wherein said authentication apparatus holds the common key and a private key used in a public-key encryption method, the authentication method comprising the steps of:

receiving a first data item, wherein the first data item is associated with a first authentication request from the server;

performing, only when the data holding medium has been authenticated in response to the first authentication request, processing for authenticating the data holding medium by a public-key encryption method, wherein the processing includes encrypting the first data item using a private-key of the user and sending the encrypted first data item to the server, wherein the server decrypts the encrypted first data item using a public-key of the user and compares the decryption result with the first data item;

authenticating, in response to an additional authentication request sent form the server to perform a service to the user, the data holding medium by using the common key used in common-key encryption method for the user held by the data holding medium, ~~and for, only when the data holding medium has been authenticated, by using the common keys~~; and

performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys in response to the additional authentication request, wherein information encrypted by the public-key encryption method is sent from the server, forwarded to the authentication apparatus, and decrypted by the authentication device using the private key corresponding to the user so as to obtain decrypted information;

wherein the decrypted information is encrypted ~~means~~ using the common key; and

wherein the obtained common key encrypted information is sent back to the data holding medium.

Claim 23 (currently amended): An authentication apparatus, comprising:

a holding means for holding a common key ~~unique to~~ corresponding to a user, used in a common-key encryption method for authentication between a data holding medium held by the user and the authentication apparatus, said holding means holding a private key used in a public-key encryption method for authentication between the data holding medium and a server to perform a service to the user;

means for authenticating wherein said means for authenticating is configured to receive a first data item, wherein the first data item is associated with a first authentication request from said server, and wherein said means for authenticating is configured to authenticate the data holding medium by using the common key in response to the first authentication request;

wherein said means for authenticating is further configured to encrypt, only if the data holding medium is authenticated in response to the first authentication request, the first data item using the private key associated with the user and to send the encrypted first data item to the server;

wherein said server is configured to decrypt the encrypted first data item using a public key associated with the user and to compare the decrypted result with the first data item;

wherein the means for authenticating is further configured to authenticate the data holding medium in response to an additional authentication request by using the common key used in common-key encryption method for the user held by the data holding medium, wherein the additional authentication request is sent only if the decrypted result corresponds to the first data item

wherein the means for authenticating is figured configured, ~~and~~ for, only when the data holding medium has been authenticated, by using the common keys, in response to the additional authentication request sent from the server, ~~said authenticating means~~ the means for authenticating being further configured for performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys,

wherein, as part of the means for authenticating performing the processing, information encrypted by the public-key encryption method is sent from the server, forwarded to the authentication apparatus, and decrypted by the authentication device using the private key corresponding to the user so as to obtain decrypted information;

wherein the decrypted information is encrypted ~~means~~ using the common key; and

wherein the obtained common key encrypted information is sent back to the data holding medium.